Deutscher Bundestag
13. Wahlperiode

Drucksache 13/1889

29. 06. 95

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Gerald Häfner, Simone Probst und der Fraktion BÜNDNIS 90/DIE GRÜNEN
— Drucksache 13/1676 —

Überlegungen der Bundesregierung zur Verschlüsselung von Daten in der Telekommunikation

Die Entwicklung neuer Techniken und Systeme im Bereich der Telekommunikation schreitet rasch voran. Nicht immer gelingt es Gesetzgebung und Recht, damit Schritt zu halten. Angesichts der Bandbreite der Anwendung moderner Telekommunikationssysteme im heutigen Leben und der Sensibilität vieler dort übermittelter Daten kommt der Entwicklung geeigneter Verschlüsselungsverfahren eine immer größere Bedeutung zu.

Der Anwendung effektiver und technisch hochwertiger Verschlüsselungsverfahren steht jedoch die Angst von Teilen der Sicherheitsbehörden entgegen, die befürchten, daß ihnen so die Möglichkeiten zum Abhören und Überwachen im Bereich der Telefon-, Fax- und Datenkommunikation verlorengehen. Es werden deshalb immer öfter Überlegungen angestellt, nur solche Verschlüsselungsverfahren zuzulassen, die entweder durch Krypto-Experten der Sicherheitsbehörden gebrochen werden können oder für die die Verschlüsselungsschlüssel in zentralen Datenbanken abgespeichert und bei Bedarf bzw. auf Anordnung an die Behörden weitergegeben werden.

1. Bisher gab es keine gesetzliche Reglementierung für den Einsatz von Verschlüsselungsverfahren. Will die Bundesregierung diesen Rechtszustand beibehalten oder plant sie eine einschränkende Regelung, z. B. in der Form eines Krypto-Gesetzes?

Die Bundesregierung prüft das Erfordernis einer rechtlichen Regelung des Einsatzes von Verschlüsselungsverfahren. Diese Prüfung ist bislang noch nicht abgeschlossen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 27. Juni 1995 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

2. Wie beurteilt die Bundesregierung in diesem Zusammenhang die sogenannte „Clipper-Initiative" der gegenwärtigen amerikanischen Bundesregierung zum Einsatz von Verschlüsselungsverfahren bei der elektronischen Übermittlung von Informationen, und sieht sie darin ein Vorbild für ähnliche Regelungen im bundesdeutschen Rechtsgebiet?

Die Bundesregierung hat diese Frage im Rahmen der 33. Sitzung des Deutschen Bundestages am 26. April 1995 bereits beantwortet (s. Plenarprotokoll 13/33, S. 2673).

3. Gedenkt die Bundesregierung Maßnahmen zu ergreifen, um die Vertraulichkeit bei der elektronischen Übermittlung von Daten und im Telefonverkehr für die Geschäfts- und Privatkommunikation sicherzustellen?

4. Wenn ja: Welche verschiedenen Maßnahmen hat die Bundesregierung erwogen, und mit welchem Ergebnis?

Die Sicherstellung der Vertraulichkeit von Telekommunikation und elektronischer Datenübertragung ist für alle Bereiche von Staat und Gesellschaft von Wichtigkeit. Die Bundesregierung plant keine besonderen Regelungen speziell für Geschäfts- und Privatkommunikation.

5. Wäre der Einsatz von Verschlüsselungsverfahren, die auch den eventuellen Zugriff von Sicherheitsbehörden auf den Nachrichteninhalt verhindern, nach Auffassung der Bundesregierung rechtlich und tatsächlich zu beanstanden bzw. unerwünscht?

Der zunehmende Einsatz von Verschlüsselungsverfahren erschwert die Arbeit der Strafverfolgungs- und Sicherheitsbehörden bei der Verbrechensbekämpfung. Im übrigen wird auf die Antwort zu Frage 1 verwiesen.

6. Wären nach Auffassung der Bundesregierung derartige Sicherheitsdienstleistungen und Kryptosysteme in öffentlichen Telekommunikationsnetzen wie z. B. dem Telefonnetz der Bundespost heute bzw. nach der geplanten Aufhebung des Monopols der Telekom beim Telefondienst 1998 zulässig?

Ja.

7. Welche Nachteile gehen nach Auffassung der Bundesregierung von der Einführung entsprechender Sicherheitssysteme aus?

Verschlüsselungsverfahren, die den legalen Zugriff von Sicherheits- und Strafverfolgungsbehörden auf den Nachrichteninhalt verhindern, wirken sich erschwerend und damit nachteilig auf die Arbeit dieser Behörden aus.

8. Welche Vorteile und welche Nachteile sprechen aus Sicht der Bundesregierung für bzw. gegen eine Reglementierung des Einsatzes von Verschlüsselungsverfahren?

Es wird auf die Antwort zu Frage 1 verwiesen.

9. Verfahren wie die Steganographie machen es schon heute möglich, verschlüsselte Daten während Telekommunikationsverbindungen so zu übertragen, daß der verschlüsselte Datenstrom nicht mehr vom „Rauschen" des Gesprächshintergrundes zu unterscheiden ist. Welche Möglichkeit sieht die Bundesregierung vor diesem Hintergrund, ein eventuelles Verbot von Verschlüsselungsverfahren auch tatsächlich durchzusetzen?

Ein Verfahren wie das der Steganografie dient der Maskierung von Nachrichten. Dabei ist es unerheblich, ob die übertragenen Informationen in verschlüsselter oder unverschlüsselter Form übermittelt werden. Im übrigen wird auf die Antwort zu Frage 1 verwiesen.

10. Wie beurteilt die Bundesregierung die Auffassung, daß das Unterlaufen entsprechender Regelungen gerade für die vielzitierte „Organisierte Kriminalität" ohne größere Probleme möglich wäre?

Verbotsregelungen unterliegen grundsätzlich der Gefahr, unterlaufen werden zu können. Dies trifft auch für ein eventuelles Verbot von Verschlüsselungsverfahren zu. Entsprechende Sanktionsnormen können aber Abschreckungswirkung entfalten.

11. Wie will die Bundesregierung erkennen, ob, wann und von wem die eventuelle Regelung eines derartigen Verschlüsselungssystems tatsächlich eingehalten wurde?

Die Beantwortung dieser Frage setzt voraus, daß Art und Umfang einer eventuellen Regelung des Einsatzes von Verschlüsselungsverfahren bereits festgelegt sind. Da die Bundesregierung momentan das Erfordernis einer solchen Regelung prüft und diese Prüfung bislang noch nicht abgeschlossen ist, kann die Frage nicht beantwortet werden.

12. Wie beurteilt die Bundesregierung die häufig vertretene Auffassung, wonach das eventuelle Verbot und die Genehmigung von Verschlüsselungsverfahren unter dem Vorbehalt des staatlichen Zugriffs das potentiell in Datensystemen erreichbare Sicherheitsniveau nicht etwa verbessern, sondern verringern würde?

Der Bundesregierung ist diese Auffassung weder bekannt noch wird sie von ihr geteilt.

13. Wie beurteilt die Bundesregierung die häufig vertretene Auffassung, daß auch die mögliche Sammlung von Schlüsseln für alle denkbaren Sicherheitssysteme einen zusätzlichen Anreiz für Hacker und Angriffe von Insidern schaffen würden?

Für die bereits heute in breitem Rahmen eingesetzten „Schlüsselsammlungen" wie z. B. im Bankenbereich liegen der Bundesregierung keine Erkenntnisse vor, daß sie sich hinsichtlich ihrer Sicherheit nicht bewährt haben sollten. Die dort erprobten Sicherheitsstrukturen könnten auch auf andere Anwendungsgebiete übertragbar sein.

14. Wie beurteilt die Bundesregierung die verbreitete Sorge, daß die Möglichkeit zur rechnergestützten Auswertung von Telefongesprächen den damit befaßten bzw. hierzu berechtigten Stellen ein erhebliches Überwachungspotential in die Hände gibt, wie beurteilt sie die Möglichkeit eines Mißbrauchs solcher Daten und wie stellt sich die Bundesregierung zu der Befürchtung, daß diese Möglichkeiten z. B. unter veränderten politischen Bedingungen zu einer sehr weitgehenden Überwachung der Bürgerinnen und Bürger genutzt werden könnte?

Die Überwachung des Fernmeldeverkehrs ist gesetzlich geregelt. Die hierzu berechtigten Stellen unterliegen einer strengen Kontrolle durch Parlament und Regierung. Es bestehen nach Auffassung der Bundesregierung keine Zweifel an der Wirksamkeit dieser Kontrollmechanismen.

15. Welche Möglichkeiten sieht die Bundesregierung, angesichts dieser Mißbrauchsmöglichkeiten, die Persönlichkeitsrechte der Bürger zu schützen und eine mißbräuchliche Verwendung auszuschließen?

Es wird auf die Antwort zu Frage 14 verwiesen.

Druck: Thenée Druck, 53113 Bonn, Telefon 91781-0
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333